ARAT Bulletin

Electronic Combat

April 1999
Volume 5, Issue 1

"Serving the Army Reprogramming Community Since 1994"

Inside this Issue

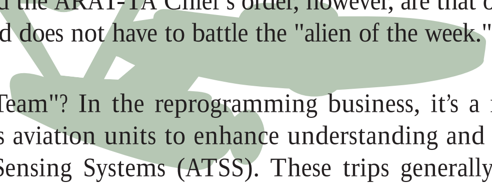
The Quarterly Professional Bulletin Published by the Army Reprogramming Analysis Team — Project Office (CECOM Software Engineering Center)

ARAT-TA Update

"Assemble the Away Team!"

By Jim Harrison, SRI International and Norm Svarrer, ARAT-TA

Star Trek fans will recognize the title phrase as one of Captain James T. Kirk's favorite commands. Recall also that team members departing the USS Enterprise soon encounter (and overcome) some sinister, alien threat. Members of the Army Reprogramming Analysis Team have become accustomed to hearing the same instructions for ARAT's Away Team from the Threat Analysis Team Chief. The two big differences between Captain Kirk's order and the ARAT-TA Chief's order, however, are that our Away Team deploys to friendly turf and does not have to battle the "alien of the week."



So, what is an ARAT "Away Team"? In the reprogramming business, it's a mission-tailored contact team that visits aviation units to enhance understanding and effective employment of Army Target Sensing Systems (ATSS). These trips generally are the result of a formal request initiated by a Command or an informal request from an Electronic Warfare Officer (EWO) who wishes to improve a unit's survivability and

See "Away Team" on page 11

Final Versions, Beta Versions Coming in Summer 1999

By Jim Holland, SRI International

The ARAT Project Office has received a lot of e-mail and phone calls about the Electronic Warfare Officer Support Software (EWOSS) and updates to the current MLV software. Here is the current status:

MLV SOFTWARE — The current MLV software distributed with the AN/APR-39A(V)1 reprogramming kit is being updated to address user comments from the field and to take advantage of the new processor capabilities of the Pentium II™ and Pentium III™ processors. At this time, MDS software is certified for use with i386™, i486™, Pentium™, and Pentium/MMX™ processor computers. Keep in mind that the MLV software has several "fail-safe" features. If an error occurs before the MDS write-verification test is completed, the active MDS is not replaced. An MDS update failure prior to the completion of the verification phase will not affect operation of the Radar Signal Detection System (RSDS) or its currently loaded MDS software. If you experience a problem using the MLV software, report it immediately.

See "Software Update" on page 9

From the Project Officer's Desk

"Self-Analysis" Clarifies Support to the Warfighter

By Joseph Ingrao, ARAT Project Officer

If an organization wants to remain effective, it must continually revisit its core competencies and match them to the needs of its customers—in our case, the Warfighters. At the ARAT/ Electronic Combat Office, we have just reviewed our core disciplines and have attempted to optimize or "fine tune" them to the needs of our customers. During this self-analysis, it became evident that ARAT/Electronic Combat, through its rapid reprogramming infrastructure, provides five major functions to the Warfighters:

FLAGGING MODELS DEVELOPMENT — An automated method of analyzing intelligence threat data (in near-real time) and directing to your threat/system analyst the pertinent information that will affect your system.

THREAT ANALYSIS — Continual monitoring of the location and changing radar signature of enemy threats. Using these data, our threat analysts will compile a tailored threat list for your EW system based on your system's capabilities, the platform, and the geographical location of the mission. Our analysts work in a Multi-service environment where they have access to and compare data with the U.S. Air Force, Navy, and Marine Corps.

MDS DEVELOPMENT, TESTING — Creation and validation of regionalized Mission Data Sets for specific EW systems. During this phase, the threat lists compiled in the previous phase are programmed into the EW system. Once the programming is completed, the system is tested using threat simulators to mimic battlefield conditions.

DATA DISTRIBUTION/FIELDING/COMMUNICATIONS — Providing a communications infrastructure to enable the Electronic Warfare Officers (EWO), or field user, to communicate as well as get the validated MDS to load into their systems. This infrastructure includes access to the Multi-Service Electronic Warfare Bulletin Board System (MSEWBBS) or the Multi-Service ARAT web site via STU-III or SIPRNET connections.

FIELD DATA LOADING — Identifying the hardware (i.e., Memory Loader/Verifier [MLV]) and developing the software to support loading the MDS into Target Sensing Systems in the field. This function also includes providing an interim rapid reprogramming capability to the Warfighter in the form of a reprogramming kit.

These processes are in-place today—they are not part of some futuristic plan. If you have questions about how our core competencies can benefit your EW system, please e-mail or call us. ◣

Frames and Search Engine Contribute to New Look at the ARAT Web Sites

By Marc C. Demarest, L-3 Communications Corp. - Ilex Systems

Greetings! If you have visited the ARAT unclassified web site recently, you may have noticed that it has a new look. This new look is very similar to the way the new classified site will look on SIPRNET. The sites have been redesigned to help make them easier to navigate and find information. The classified web site will have some added features as well.

One new feature of these sites is the use of window frames, which require an HTML version 3.2-compliant browser (i.e., Netscape 3.x or higher, Internet Explorer 3.x or higher). Frames were used so that at all times you can go elsewhere within the web site quickly and easily. For example, if you are reading an online version of the *ARAT Bulletin* on the SIPRNET web site and wish to go to the Mission Data Set area, you can just click on the "Mission Data Sets" link in the window located on the left. We are also trying to give you, in the field, more information as it becomes available. We are separating this information into as many logical areas as possible so it will be easier for you to find the information you need.

Continued on page 10

ECB's "TAG-Team" Process Streamlines Threat Analysis Efforts

By Armando Torres, Ilex Systems

The Electronic Combat Branch (ECB) of the Communications-Electronics Command (CECOM) Software Engineering Center (SEC), located at Fort Monmouth, NJ, develops domestic and Foreign Military Sales (FMS) Mission Data Sets (MDSs) for the AN/APR-39 series of Radar Signal Detecting Sets (RSDSs). This article describes a change in the approach to the threat analysis portion of the ECB mission. The Threat Analysis Group (a.k.a., TAG-Team) concept, which is introduced in this article, is a step towards improving efficiency by eliminating duplication of effort.

The ECB is divided into separate teams for MDS development for each of the AN/APR-39 series RSDSs [-A(V)1/3, -A(V)2, and -(V)2], as well as a team for the Advanced Multiple Environment Simulator (AMES). In the past, MDS development and test procedures for each system, and for the AMES, involved independent analysis of threat emitters by each system's programmers and the simulation engineers. This process was followed by development of the actual MDS and corresponding threat simulation(s).

While both ECB and ARAT-TA conduct independent analysis of the threat emitters, the type of analysis differs between the two. The analysis performed by ARAT-TA, which is of a more general nature, consists of the following steps:

- Determine system for reprogramming
- Determine country or region of employment
- Identify all radars in that country or region
- Determine threat radars in that country or region
- Obtain/analyze threat parameters
- Designate the parameters to be reprogrammed

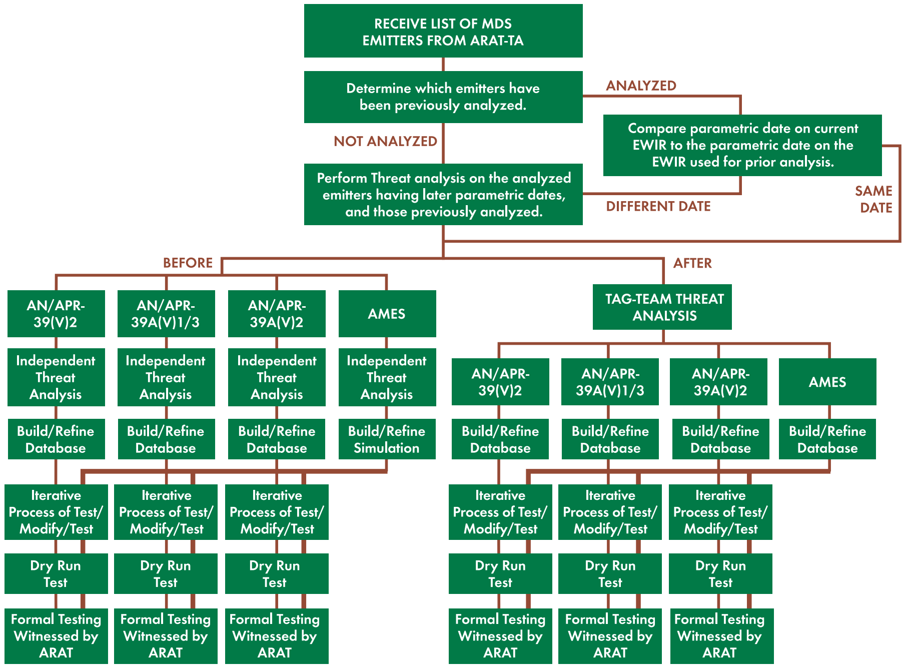
Before the TAG-Team was established, ECB's processes and procedures resulted in a duplication of effort during the analysis phase of the MDS development. It also caused some degree of confusion among the teams when analyzing the same threat data—a result of the differences in each team's approach to analyzing threats, based on the variations in the system requirements. A more efficient method was needed to improve the way the ECB accomplished its mission. This new method involved development of the TAG-Team. The TAG-Team includes representatives from each -39 system team, as well as simulation engineers, making the overall TAG-Team's method of analysis uniform to development and testing of all -39 systems.

Characteristics of TAG-Team

- Composed of developers and testers from each -39 system
- Basic analysis not limited to the requirements of any one particular system
- Review and verification process-instituted work
- Structured meeting time and analysis formats

The job of the TAG-Team is to analyze, in a concerted effort, various databases (e.g., EWIR, KILTING) for use by any of the system's teams to develop MDSs and for creation of simulation threat libraries. The basic analysis that the TAG-Team performs includes extracting parameters from the databases, performing calculations to aid emitter mode creation, and listing the relevant data and suffix codes in a standardized format. This approach not only eliminates duplication of effort, it also provides a single reporting format, designed by the developers and testers, to incorporate the requirements of each system into the overall effort. The TAG-Team meets every morning, Monday – Thursday, as MDS development efforts require, and holds a verification and review session on Friday. The MDS development process is illustrated below.

Continued on page 9


RECEIVE LIST OF MDS EMITTERS FROM ARAT-TA
Determine which emitters have been previously analyzed.
ANALYZED
Compare parametric date on current EWIR to the parametric date on the EWIR used for prior analysis.
NOT ANALYZED
Perform Threat analysis on the analyzed emitters having later parametric dates, and those previously analyzed.
DIFFERENT DATE
SAME DATE
BEFORE
AFTER
AN/APR-39(V)2
AN/APR-39A(V)1/3
AN/APR-39A(V)2
AMES
TAG-TEAM THREAT ANALYSIS
Independent Threat Analysis
Independent Threat Analysis
Independent Threat Analysis
Independent Threat Analysis
AN/APR-39(V)2
AN/APR-39A(V)1/3
AN/APR-39A(V)2
AMES
Build/Refine Database
Build/Refine Database
Build/Refine Database
Build/Refine Simulation
Build/Refine Database
Build/Refine Database
Build/Refine Database
Build/Refine Database
Iterative Process of Test/ Modify/Test
Iterative Process of Test/ Modify/Test
Iterative Process of Test/ Modify/Test
Iterative Process of Test/ Modify/Test
Iterative Process of Test/ Modify/Test
Iterative Process of Test/ Modify/Test
Dry Run Test
Dry Run Test
Dry Run Test
Dry Run Test
Dry Run Test
Dry Run Test
Formal Testing Witnessed by ARAT
Formal Testing Witnessed by ARAT
Formal Testing Witnessed by ARAT
Formal Testing Witnessed by ARAT
Formal Testing Witnessed by ARAT
Formal Testing Witnessed by ARAT

Y2K-Compliant Software Installed and Tested on GRCS Systems

By Raymond Santiago, Countermeasures Systems Branch (SED)

Last year in Taszar, Hungary—in support of the Program Executive Office, Intelligence, Electronic Warfare and Sensors, and the Program Manager, Signals Warfare—personnel from the Software Engineering Center (SEC) Guardrail Common Sensor (GRCS) program successfully installed and tested Year 2000 (Y2K) software on Guardrail systems. Taszar, an active Hungarian airbase about 40 miles from the Croatian border, supports NATO operations.

The Guardrail team upgraded and installed Y2K-compliant software on the GRCS System 4, which is assigned to the 1st MI Battalion, then conducted mission analysis testing by setting the time before and after the Year 2000 to observe the software's performance. Before installing the Y2K-compliant hardware and software to System 4 workstations, the team backed up all affected software programs. Next, System Test Dates (STD) tests were exercised to determine if any mission functions or operations were affected by the changes. During the test cycle, the team examined Y2K operations test (OT) procedures, which verified acceptance of critical rollover dates on the Guardrail system. The test dates were set one hour before and one hour after the Year 2000 (to test for Y2K acceptance) and from February 28 to 29 of the Year 2000 (to test for leap year acceptance). Other tests were conducted to include the Year 2001 to verify that the entire year rollover date would be accepted. The upgrades and software installation were scheduled around the mission so no degradation in support to NATO forces would occur. Assigned military personnel operated the system workstations as Guardrail personnel monitored the operations. All personnel worked around the clock, in two shifts, so support to normal mission requirements would not be affected.

GRCS is a family of tactical signal and direction-finding (DF) intercept systems whose mission is to locate, identify, and communicate information on hostile emitters to tactical commanders. Common Sensor Systems consist of several configurations and are deployed worldwide to support tactical forces—GRCS System 1 is deployed with the 224th MI Battalion at Savannah, GA; System 3 supports the 3rd MI Battalion in Korea; System 4 is located with the 1st MI Battalion in both Germany and Hungary; and Improved Guardrail V (IGRV) is located with the 15th MI Battalion in Fort Hood, TX. A Guardrail training system, USAIC, is located at Fort Huachuca, AZ.

The Guardrail fielding team—which consisted of Government engineers, ILEX engineers, and associated contractor engineers from Cardinal Information Solutions (CIR), Creative Computer Solutions (CCS), Advanced System Technology, Inc., (AST), and Galaxy (subcontractor to TELOS Systems Group)—is to be commended for the excellent work done in meeting the first of many Y2K challenges. Systems 1 and 3 were also successfully upgraded in 1998, and IGRV was successfully upgraded in March 1999. The leadership and direction of LTC Harold Greene, the Product Manager Aerial Common Sensor (ACS), Mr. Joseph Matava, the Product Manager GRCS, and MAJ Stephen Winter were instrumental in the success of this program.

Special Feature

Information Warfare Friendly Fire: A New Concept in IO

By Carl Brunner, SRI International

Many people have experienced failure of automated systems when they were needed most. But frequently the failure is not a hardware or software problem—it is the result of other people's actions. Actions taken to improve capabilities sometimes produce the opposite effect. The planned upgrade diminishes capability because of faulty planning or implementation. Few things are as frustrating to users or have a greater potential for disaster. Here is a sample of how problems can occur.

> An Army contractor is completing a proposal and requires one final piece of information from the home office to meet the tight deadline. The entire package has to go to the binder in 30 minutes to guarantee delivery in time to submit the proposal. The final information comes across the modem after 20 minutes on a mediocre phone connection. The contractor opens the file to cut and paste it into the proposal, but the document on the screen appears to contain nothing but an array of small rectangles. Oh no! A panicked phone call to the home office reveals the problem. The home office upgraded to Office97™ yesterday and his copy of the software will be mailed out today. In the meantime, the home office will send the file in the old format in an e-mail. The result? No delivery guarantee from the binder. And no guarantee the contractor will have a job if the proposal isn't delivered by the deadline.

The plight of this contractor illustrates how information systems are subject to human failure and shows how the results of such an oversight can be devastating to the mission. Although this example is not particularly catastrophic, such a failure could easily happen to troops in the field where the consequences could be deadly.

Human failure in automated information systems is an important consideration, given the increasing number of weapons and C3 systems that rely on them. Without information, the Army's ability to conduct effective operations is restricted and the ability to defeat large enemy forces with smaller, highly dynamic friendly forces is lost. Recognition of this situation brought about the concept of Information Warfare and Information Operations. We recognize the value of information, so we protect our ability to gather and process it while we attempt to disrupt the enemy's information systems. But where do we address the human errors like the one illustrated above? When such failures occur, we injure our own ability to process information. We are doing the enemy's job for him. This concept has not been addressed adequately in Information Operations. We should refer to this self-inflicted damage to our information systems as what it really is: Information Warfare Friendly Fire.

Friendly fire is a strong term to use. In recent conflicts, friendly fire has caused nearly as many casualties as enemy fire and has become unacceptable in the U.S. military. In a similar fashion, we have a much greater ability to damage our own information systems than most of our enemies ever will. Given our reliance on information systems to conduct combat operations, we should treat Information Warfare Friendly Fire (IWFF) with the same degree of seriousness as that given to friendly fire involving weapons. In the end, IWFF could be more catastrophic and expose more troops to harm than does friendly weapons fire. Given the information automation anticipated in Army XXI, IWFF could easily lead to friendly fire incidents in the future.

Information Warfare Friendly Fire occurs on a daily basis in a variety of forms. Every job that uses automated information systems, which encompasses almost every operational and support function in the Army, is vulnerable to oversights that can turn information systems into obstacles instead of tools. The example above shows how software upgrades can become a problem. If not implemented uniformly, software upgrades can eliminate some users from the communications network more effectively than could any enemy. Here are other examples that show the variety of environments in which IWFF can happen:

▶ **Software implementation that is not adequately tested and debugged.** Insufficiently tested software can have minor functional failures or it can crash outright. In either case, units in the field lose their intended utility.

▶ **Eliminating redundancy in information systems.** To promote efficiency, some system administrators remove older systems as new replacement systems come online. However, if the primary system fails, it is nice to have a backup system for critical applications. For reprogramming actions, access to the Multi-Service Electronic Warfare Bulletin Board System (the MSEWBBS) is critical. The SIPRNET has made access to the MSEWBBS very fast, but occasionally the SIPRNET line goes down for extended periods. The reprogramming flagging shop maintains the STU-III dial-up capability as a backup to the SIPRNET, even though it is much less capable.

▶ **EW systems that were procured without a rapid reprogramming capability.** Electronic threat systems are extremely dynamic. If an EW system is not capable of accommodating the parametric changes of threats, it will have marginal utility by the end of the first day of the war.

▶ **Communications systems with insufficient baud rates.** Many Army information systems use commercial software. As new machines have become available with greater processing and storage capability, file sizes have grown to take advantage of new software features. For secure file transmission, the STU-III is the standard equipment throughout DoD. However, the STU-III doesn't do much better than a 9600-baud rate, so sending a 30-slide PowerPoint97™ briefing across a phone

Continued on page 11

ARAT Project Supports Operational, R&D, and Other Systems

By Jim Holland and Jim Harrison, SRI International

The Army Reprogramming Analysis Team (ARAT) project is tasked by the Department of the Army to provide threat analysis, software reprogramming, and software installation assistance for Army Target Sensing Systems (ATSS). Since 1992, ARAT has evaluated existing and developmental weapons systems across combat arms and combat service support functional areas. The purpose of this evaluation has been to identify ATSS that use signatures-based software for recognition, classification, countermeasures, and targeting functions, and to provide assistance as necessary.

ARAT now provides threat analysis and software reprogramming support for eleven (11) ATSS, and is assisting with other systems still in the research and development (R&D) phase. In addition, ARAT provides occasional support to other weapons systems that do not strictly meet ATSS definitions. Initially, ARAT provided support primarily to the aviation community. However, with the introduction of additional signatures-based sensors and weapons, ARAT is now involved across service and functional boundaries to provide operational and R&D assistance.

This article provides only system names and a brief description of the ARAT support provided for those systems. Readers with questions on specific system capabilities, or detailed information on ARAT support, should contact the ARAT Project Office directly. Table 1 reflects ARAT support to fielded systems. Table 2 reflects ARAT support to systems in development.

Operational Systems Support

Support for currently fielded weapons systems is operationally oriented to ensure that the Warfighter has the best data in the system when it is employed. Emphasis has been placed on developing regional data loads that contain targets and threats in current operations areas. This regional approach tailors the system to what it may encounter, greatly improving system performance.

Any unit using ATSS is authorized to contact ARAT-TA directly for assistance in selecting the best Mission Data Set (MDS) for use, or to request new data sets to meet unit operational requirements.

Continued on page 7

Table 1: OPERATIONAL SYSTEMS

Weapon Systems	ARAT Support	Notes
AN/APR-39A(V)1 RSDS	Threat Analysis, Intelligence Flagging, Software Reprogramming and Testing, Software Distribution, Systems Engineering, Memory Loader Verifier Kit	MLV Kit and Software Available
AN/APR-39A(V)2 RSDS	Threat Analysis, Intelligence Flagging, Software Reprogramming and Testing, Software Distribution, Systems Engineering, Memory Loader Verifier Kit	MLV Kit and Software in Development
AN/AVR-2A Laser Detection Set	Threat Analysis, Software Reprogramming and Testing, Software Distribution, Systems Engineering	
AN/ALQ-136 Electronic Countermeasure	Threat Analysis	Limited Software Reprogramming Possible

Continued from page 6

R&D Systems Support

ARAT assists TRADOC Schools and Centers, Army Material Command (AMC), and Program Managers (PM) during ATSS R&D. Assistance provided includes threat signature data analysis and systems engineering for software programming, unit-level software installation, and system testing.

Weapons systems that will be fielded after the Year 2000 will bring ATSS into widespread use across the battlefield. One area that will require significant resources is the development of combat vehicle survivability systems. The large quantities of systems—and diverse locations where they will be employed—will significantly increase the need for a responsive support capability, dwarfing what is now required by the aviation community. Systems listed in Table 2 are receiving ARAT support during R&D.

Table 2: R&D SYSTEMS

Weapons System	ARAT Support	Notes
AN/ALQ-212 Suite of Integrated IR Countermeasures (SIIRCM)	Threat Analysis, Intelligence Flagging, Software Reprogramming and Testing	ASE for Helicopters and Fixed-Wing aircraft
AN/APR-48 Radio Frequency Interferometer	Threat Analysis, Intelligence Flagging, Software Reprogramming and Testing, Software Distribution, Systems Engineering	ECP to Enhance Unit-Level Software Reprogramming Capability

Potential Systems Support

ARAT plays a significant role in Army development and exploitation of signatures data for aviation electronic combat (AEC) systems. Lessons learned from the AEC experience and reprogramming infrastructure initiatives argue that the ARAT process has considerable application in other functional areas—i.e., air defense, fire support, intelligence, and signature database efforts (see Table 3).

Table 3: ATSS-POTENTIAL SYSTEM SUPPORT

System	ARAT Support	Notes
Patriot Air Defense System	Signature Analysis, Database Development	
Smart Munitions	Signature Analysis, Database Development, Systems Engineering	Includes WAM, SADARM, and BAT
National Target/Threat Signature Data System (NTSDS)	Assist in Database Development, Systems Engineering, Army Site Modernization for NTSDS Host and User Services	
EW Integrated Reprogramming Database (EWIR)	Database Development, Systems Engineering, EWIR Data Format and Distribution Improvements	Includes Efforts for EWIR Database Software and Analyst Tool
Army TSS Software Test Facilities	Systems Engineering, Systems Modernization	

Conclusion

Since its inception, ARAT has aggressively pursued its mandate from the Army Staff to provide ATSS reprogramming assistance to the Warfighter and R&D communities. The operational systems ARAT supports are used on thousands of platforms and by all U.S. services and several Allied nations to provide identification, countermeasure, and targeting functions. In the near future, even more-complex systems will be fielded and used more commonly than ever before. The ARAT Project is working today to ensure that the Warfighter has what is needed to fight when these systems are deployed in the future. ◣

NTSDS SiDDWG Update

By Jim Holland, SRI International

Since its activation in 1991, the ARAT Project has been providing support to Army Target Sensing Systems (ATSS) that use Measurement and Signatures Intelligence (MASINT) information. Central to MASINT collection and distribution efforts for the United States is the National Target/Threat Signature Data System (NTSDS), managed by the National Ground Intelligence Center (NGIC).

NTSDS is a distributed MASINT data repository and analysis system accessible using the Secure Internet Protocol Network (SIPRNET) and Joint Worldwide Intelligence Communications Network (JWICS). As part of the development of the NTSDS, NGIC also started the Signatures Data Development Working Group (SiDDWG), a forum for MASINT data users and collectors to exchange information.

The SiDDWG meets annually in conjunction with an NTSDS progress review to discuss emerging signature data collection and analysis methods and technologies. For the past three years, the ARAT Project Office provided funding for the SiDDWG chairman, Jim Holland (SRI International). During these years, presentations featured topics such as:

- Computer modeling advances for rapid development of millimeter-wave and thermal signatures for ground and missile targets, based on images and physical measurements
- Advances in measurement of radar cross sections for conventional and low-observable targets
- Advances in development of computer model and range targets to simulate threat ballistic and cruise missile targets
- Innovations in non-cooperative target recognition
- Methods for detection of targets in clutter for application to search and rescue

Chairmanship of the SiDDWG has been passed this year to Mr. Mark Minardi, who works in the Sensors Directorate, Air Force Research Laboratory, at Wright Patterson AFB, OH. Upcoming SiDDWG sessions are expected to focus on subjects such as automatic target recognition technologies and the signature data necessary to support future weapons systems. Warfighters and other users of MASINT signature data are encouraged to attend the SiDDWG sessions to learn more about the national capabilities available to exploit signature data.

The ARAT Project has supported the NTSDS effort since 1992, and will remain involved with MASINT collection and analysis well into the future. The ARAT Project thanks Jim Holland for his efforts and wishes Mark Minardi the best for the upcoming year.

MASINT-based ATSS use multi-spectral signature information to perform detection, classification, countermeasure and engagement tasks. Examples of Army MASINT-based ATSS in operation today include:

- AN/APG-78 Longbow Fire Control Radar—Millimeter wave radar
- AN/AVR-2A(V) and AN/VVR-1 Laser Detection Set—Laser energy detector
- AN/AAR-47 Missile Warning System—Multi-spectral missile launch event and plume tracking
- Brilliant Anti-Tank Munition (BAT)—Acoustic and thermal signature location and identification

Numerous MASINT-based systems are used in roles as varied as intruder detection, strategic missile launch warning, and nuclear weapons test monitoring. Other MASINT-based ATSS currently in development will perform a variety of roles—e.g., non-cooperative recognition and engagement of surface and air targets, active missile detection and countermeasure, fratricide prevention, vehicle survivability, and intelligence gathering operations. ◣

NTSDS/SiDDWG
Points of Contact:

William F. Reinhold
NGIC NTSDS Program Manager
DSN 934-7644
Comm. (804) 980-7644
e-mail: reinhold@ngic.osis.mil

Mark Minardi
AFRL/SNAA, SiDDWG Chairman
Comm. (937) 255-1113, ext. 2691
e-mail: mminardi@mbvlab.wpaf.af.mil

Jim Holland
SRI International
ARAT-PO
Comm. (301) 862-4507
e-mail: holland@wdc.sri.com

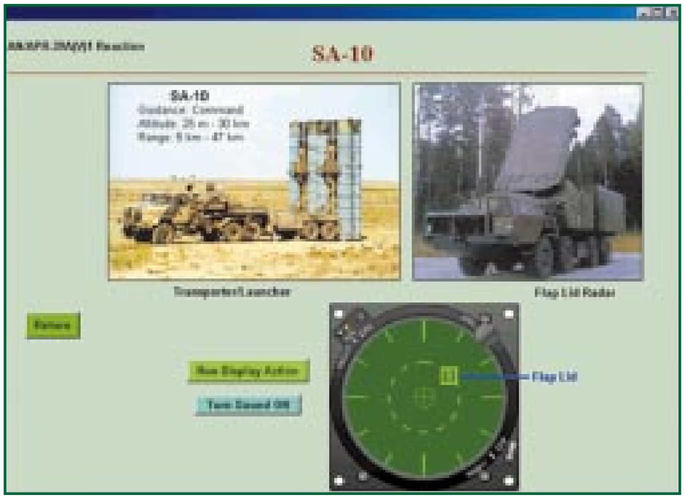
ARAT MDS Training Product

By Gray Smith, SRI International

The Army Reprogramming Analysis Team Project Office (ARAT-PO) now has the capability to create Mission Data Set (MDS) training products. Rich in multimedia content, these products are distributed on CD-ROM and are viewable on any IBM/PC-compatible system. Each training product is tailored to a specific MDS and includes emitter and threat information, as well as display representations, relative to the AN/APR-39A(V)1 signal detection set.

These products provide training via a mixture of text, graphics, pictures, animations, video, and audio. Considerable user interaction is available on almost every topic to promote a better understanding of the AN/APR-39A(V)1 capabilities and Electronic Warfare in general. A representative example is shown in the figure to the right.

An unclassified version of an MDS training product was displayed at FiestaCrow '99 in San Antonio, TX. ◣



SA-10
Guidance: Command
Altitude: 25 m - 30 km
Range: 5 km - 47 km

Software Update

Continued from page 1

A final version of the MLV software update is expected to be released in Summer 1999. A Beta release is being developed and should be available by the time this issue of the *Bulletin* is published. Contact the ARAT Project Office to receive the MLV Beta software. The final release is being delayed slightly to allow compatibility testing with the Pentium III™ processor recently introduced by Intel Corporation.

MLV software and a reprogramming kit are being developed to support the AN/APR-39A(V)2. The software is being designed to be similar in use to the current MLV program for the AN/APR-39A(V)1/3/4. The kit will include a MIL-STD-1553B bus interface (PC Card) and a special-purpose cable. Cost and availability have not yet been determined. Look for details in the next *Bulletin*.

EWOSS SOFTWARE — A new version of the EWOSS will be released after the MLV software is completed. Updates to the EWOSS will include the ability to use either Netscape™ or Internet Explorer™ based on the system's default browser configuration. The new MLV software will be incorporated into EWOSS as well, with an interface to support reprogramming sessions inside windows. The EWOSS Beta should be available by early Summer 1999. The new version of EWOSS will be distributed to all registered users of the MLV software. ◣

Laptop MLV software being used to reprogram an AN/APR-39A(V)1 in a Kiowa Warrior

Threat Analysis Update

Continued from page 3

The TAG-Team reduces the work and time that each system's team would put into re-analyzing the same threat data. Based on the efforts of the TAG-Team, each system team then refines the basic threat analysis, depending on the system's specifications and ARAT-TA's recommendations to create the program database. In addition, the test scenario generation team refines the TAG-Team's analysis and implements the emitter for simulation via the AMES. An iterative process of test and modification then takes place to bridge any abnormalities in the MDS or simulation. Finally, ECB engineers conduct a preliminary test on the completed MDS, followed by formal testing in the presence of an ARAT-TA representative. Any questions regarding the TAG-Team should be addressed to the CECOM SEC ECB. ◣

ARAT Web Sites Update

Continued from page 2

Another feature is a new search engine. This search engine, which is similar to the ones you might use when browsing other web sites, should make searching for information straightforward and the search page easy to use.

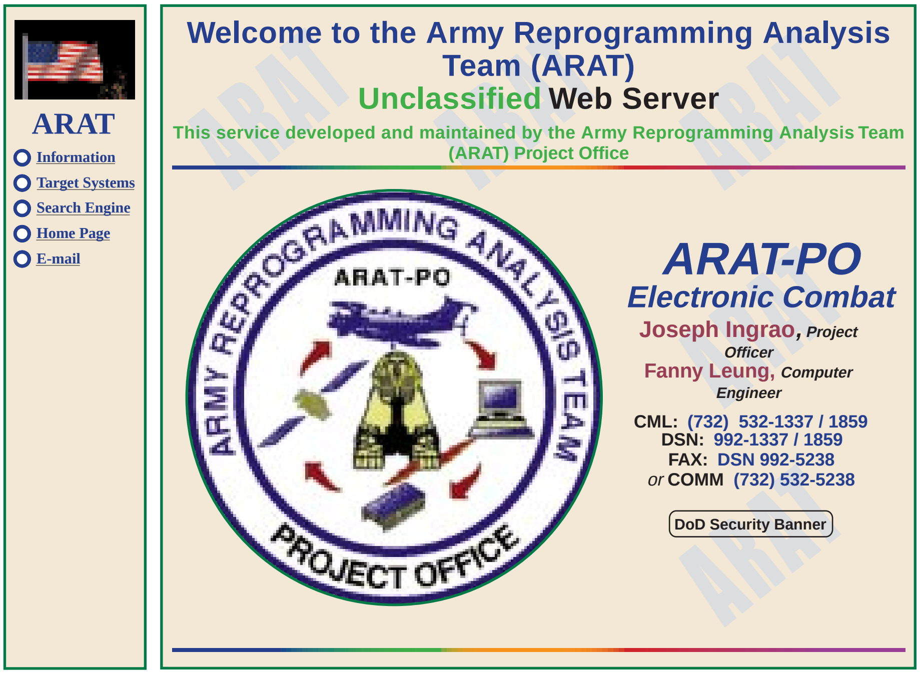
The pages will contain the following areas and types of information. The major headings listed correspond to the links you will find in the "navigation" window on the left side of your screen.

Information

- Army Reprogramming Offices—this will have information on ARAT locations and offices
- ARAT Bulletins—All past and present bulletins in Word '97, PDF, and HTML formats
- Account Application Forms
- STU-III Files
- Documentation Library
  - ARAT Mission Statement
  - ARAT Charter
  - "ARAT Technical Architecture"–SIPRNET ONLY
  - JULLS–SIPRNET ONLY
  - "Army Rapid Reprogramming Guide"–SIPRNET ONLY
  - "Warfighter Support Handbook"–SIPRNET ONLY
  - Technical Tips
  - Technical Bulletins
  - "Army Technical Architecture"–SIPRNET ONLY
- Terms Reference Guide
- General Gunther's WWW Directive

Mission Data Sets — SIPRNET ONLY

- Log on to MSEWWEB
- Telnet to MSECBBS
- ARAT FAQS



Welcome to the Army Reprogramming Analysis Team (ARAT)
Unclassified Web Server

This service developed and maintained by the Army Reprogramming Analysis Team (ARAT) Project Office

ARAT-PO
Electronic Combat
Joseph Ingrao, Project Officer
Fanny Leung, Computer Engineer

CML: (732) 532-1337 / 1859
DSN: 992-1337 / 1859
FAX: DSN 992-5238
or COMM (732) 532-5238

Exercise Activities — Multi-Service and Army Exercise Activities — SIPRNET ONLY

- Proud Byte
- Brave Byte
- Serene Byte
- Neptune Byte

Training — SIPRNET ONLY

We will be putting reprogramming-related training in this area. It will have both multimedia training and text-based training/information.

Target Sensing Systems — Various types with descriptions, pictures, and POCs

- Air Defense
- Countermobility/Survivability
- Direct Fire
- Fire Support
- Intelligence and Electronic Warfare

Search Engine

ARAT E-mail — ARAT community address list

To visit the unclassified site on the Internet, go to:

http://arat.iew.sed.monmouth.army.mil

or the classified site on SIPRNET at:

http://www.arat.army.smil.mil

Suggestions, as always, are welcome from users in the field and can be sent via e-mail to:

Internet:
webmaster@comanche.iew.sed.monmouth.army.mil

SIPRNET:
webmaster@arat.army.smil.mil ◣

"Away Team"
Continued from page 1

ARAT-TA's Jim Coots describes the ARAT process to ASE/EWO students

capabilities through better use of Aircraft Survivability Equipment (ASE). We work with the host unit to deploy a team that best meets the unit's requirements. Generally, our presentations review the capabilities, operation, and limitations of the visited unit's ASE. We also routinely demonstrate the Multi-Service Electronic Warfare Bulletin Board System (MSEWBBS) and ASE rapid reprogramming, and review Mission Data products available to aviators. Team members also discuss recent or anticipated changes in the Army Aviation's worldwide threat environment. "War stories," of course, are thrown in free of charge.

Since the first ARAT Away Team was dispatched in 1994, we have completed eight large-unit visits—two each to Ft. Campbell, Ft. Hood, and U.S. Forces Korea, and one each to Wheeler AAF and Ft. Bragg. We have also conducted similar trips to Marine Aviation Weapons and Tactics Squadron One, Navy Special Boat Squadron One, and to two Air Force Rescue Squadrons. As a result of these trips, well over 600 users and maintainers of ATSS have received the latest tips and information on the care, use, and feeding of their ASE.

Another extremely important port of call for the Away Team is nearby Ft. Rucker, AL, where the Army Aviation Center conducts approximately 12 sessions of the Aircraft Survivability Equipment/Electronic Warfare Officer (ASE/EWO) Course every year. The ASE/EWO Course is "designed to provide officers and warrant officers with the skills and knowledge necessary to supervise and manage aircraft survivability equipment training for operators, and to provide maintenance and logistics assistance." Because the course is geared toward ASE operation and reprogramming, it is the perfect opportunity for aviators to be introduced to the ARAT and its Threat Analysis Team (ARAT-TA).

Whenever schedules permit, one or two Team members make the short trek to the ASE/EWO class where they provide briefings on Threat Analysis Team functions, MDS and other products, and other assistance available to EWOs. Because many of the Course graduates will soon be assigned as unit EWOs or Tactical Operations Officers, first-hand knowledge of the Threat Analysis Team can make their jobs easier by increasing their knowledge of resources available to each of them. Since beginning our "guest speaker" program in 1997, the Threat Analysis Team has appeared before more than 250 students at the ASE/EWO Course. We consider these contacts particularly important to the future of Army ASE because the students are drawn from many ranks, experience levels, and unit types. It's always rewarding to receive positive calls or emails from unit EWOs who first learned of the Threat Analysis Team while at the ASE/EWO class.

Obviously, one of our tasks is to increase the user community's awareness of our EW support processes and products. The Away Team is our vehicle for reaching out to the units. We highly value the direct contact with Warfighters at unit visits, and the feedback provided during these visits improves our understanding, processes, and products.

Limited funding is available for Away Team support. For additional information, please contact Mr. Norm Svarrer at **DSN 872-8899**, or commercial **(850) 882-8899**. ◣

Special Feature
Continued from page 5

line can take a long time. For combat applications, that situation is unacceptable.

None of these examples cited is fictitious. It is not hard to imagine how widespread IWFF incidents are or how much effort is wasted on self-inflicted problems.

The best way to eliminate Information Warfare Friendly Fire is awareness of the information system users' needs and the consequences they would endure if they lost use of their systems. The soldiers in the field are the reason these systems exist. Their needs are paramount. Information system activities—from acquisition through fielding and maintenance—must be conducted so that the soldiers have continuous, uninterrupted access to their systems. The extent of information systems integration into operations and the pace of modern combat allow nothing less. It is incumbent upon those of us who provide information to soldiers to ensure our products provide the best capability and to do whatever is required to keep soldiers' information-based systems updated without interfering with their combat capability. ◣

ARAT Bulletin

Electronic Combat

For Your Information

Coming Events

Event	Location	Dates
Braxton-Bragg-AUSA	Fort Bragg, NC	May 1999
AAAA Annual Convention	Nashville, TN	9-12 May 1999
EW '99 Electronic Warfare	London, UK	17-18 May 1999
Joint Avionics and Weapon Systems Conference & Exhibition	San Diego, CA	14-17 June 1999

The ARAT Community — Key Points of Contact

Agency	Name/e-mail	Comm/DSN	FAX Number
HQDA, DAMO-FDI	Mr. William M. McDowell mcdowwm@hqda.army.mil	DSN 227-4257	DSN 223-5336
HQ, TRADOC	Mr. Bob Miner minerr@monroe.army.mil	(804) 727-2664 DSN 680-2664	(804) 727-3199 DSN 680-3199
HQ, INSCOM	COL James P. Gibbons jpgibbo@vulcan.belvoir.army.mil	(703) 706-1791 DSN 235-1791	(703) 806-1003 DSN 656-1003
ARAT-PO	Mr. Joseph Ingrao ingrao@mail1.monmouth.army.mil	(732) 532-1337 DSN 992-1337	(732) 532-5238 DSN 992-5238
ARAT-TA	Mr. Norm Svarrer svarrer@eglin.af.mil	(850) 882-8899	(850) 882-8213 (C) -4268 (U)
		DSN 872-8899	DSN 872-8213 (C) -4268 (U)
ARAT-SE (CECOM)	Mr. Joseph Ingrao ingrao@mail1.monmouth.army.mil	(732) 532-1337 DSN 992-1337	(732) 532-5238 DSN 992-5238
ARAT-SC (FT. RUCKER)	Mr. George Hall hallg@rucker.army.mil	DSN 558-9334	DSN 558-1165
	CW4 Steve Woods stephen_woods@rucker.army.mil	(334) 255-1861 DSN 558-1861	(334) 255-3468 DSN 558-3468
AFIWC (KELLY AFB) (Army Flagging)	LTC Robert A. Wiedower rawiedo@afiwc.aia.af.mil	(210) 977-2021 DSN 969-2021	(210) 977-2145 DSN 969-2145
	Mr. Carl Brunner carl.brunner@sdd.sri.com	(210) 977-2021 DSN 969-2021	(210) 977-2145 DSN 969-2145

The ARAT Bulletin Staff

Send comments, changes of address, and articles to:

U.S. Army CECOM
Software Engineering Center
ATTN: AMSEL-SE-WS-AI-EC
Fort Monmouth, NJ 07703-5207
FAX: 992-5238 (DSN); (732) 532-5238 (Commercial)

Editor-in-Chief
Mr. Joseph Ingrao, ARAT Project Office

Editor
Mr. Jody Brown, SRI International

Graphic Designer
Ms. Linda Axford, SRI International